



**U.S. Department of Justice**

*United States Attorney  
Southern District of New York*

The Silvio J. Mollo Building  
One Saint Andrew's Plaza  
New York, New York 10007

November 3, 2020

**UNDER SEAL**

**BY ELECTRONIC MAIL**

**MEMO ENDORSED**

The Honorable Laura Taylor Swain  
United States District Judge  
Southern District of New York  
500 Pearl Street  
New York, New York 10007  
(212) 805-0426

**Re: United States v. Gery Shalon**  
SI 15 Cr. 333 (LTS); 17 Cr. 254 (LTS)

Dear Judge Swain:

The Government respectfully submits this letter to advise the Court of the pertinent facts concerning the substantial assistance that Gery Shalon has rendered in the investigation and prosecution of other persons. In light of the facts set forth herein, and assuming that Shalon continues to comply with the terms of his cooperation agreement and commits no additional crimes before sentencing, the Government intends to move at sentencing, pursuant to Section 5K1.1 of the United States Sentencing Guidelines (the "Guidelines"), that the Court sentence Shalon in light of the factors set forth in Section 5K1.1(a)(1)-(5) of the Guidelines. Shalon is scheduled to be sentenced on December 1, 2020 at 11:00 AM.

**Factual Background and Criminal Conduct**

Gery Shalon and his Russian business partner, Vlad Kholkolkov, led and owned a vast international cybercriminal organization, with operations in Israel, Russia, Ukraine, and elsewhere. At the time of Shalon and his co-defendant Ziv Orenstein's arrest in Tel Aviv in July 2015, Shalon and Kholkolkov, who was based in Moscow, jointly owned a criminal conglomerate which conducted a variety of different criminal businesses, including online gambling and pharmaceutical<sup>1</sup> companies and brands which catered to U.S. customers;

---

<sup>1</sup> Shalon and Kholkolkov jointly owned RxPartners, one of the largest online pharmaceutical affiliate networks. RxPartners sold generic versions of patented pharmaceuticals, mainly erectile dysfunction drugs Viagra and Cialis. RxPartners had its own distribution

Honorable Laura Taylor Swain  
 November 3, 2020  
 Page 2

fraudulent payment processing which allowed for credit and debit card transactions for a variety of criminal activities (including their own gambling and pharmaceutical transactions, as well as other “high risk” lines of business); and an unlicensed Florida-based bitcoin exchange named Coin.mx.<sup>2</sup> Shalon focused on overseeing the casino and payment processing businesses, while Khokholkov focused on the pharmaceutical and bitcoin businesses. In addition, Shalon, Khokholkov, and their associates laundered hundreds of millions of dollars from their criminal activities through various international bank accounts mainly located in Cyprus, Georgia, and Switzerland. This extensive money laundering network involved at least 75 shell companies and bank and brokerage accounts located across the world.

In furtherance of these business activities, Shalon directed various cyberattacks against a variety of companies, including online gambling competitors and a U.S.-based merchant risk intelligence firm, in an effort to undermine the firm’s efforts to detect fraud and illegal activity in payment processing for major credit card networks. Separate from these business ventures, however, Shalon also organized an effort to hack into major U.S. financial institutions and financial sector businesses, in order to steal lists of customers and their contact information to use in furtherance of a securities pump-and-dump scheme. Shalon did so with the assistance of Joshua Samuel Aaron, a U.S. citizen who was living in Tel Aviv and who aided Shalon in perpetrating the securities pump-and-dumps, by selecting the penny stocks to manipulate, facilitating the publication and dissemination of materially false statements about these stocks that through spam and hard mailers (i.e., paper flyers and newsletters which were mailed to U.S. residents), and recruiting U.S.-based co-conspirators. Aaron also played a role in identifying which U.S.-based companies Shalon should target for purposes of stealing contact information. These hacks were conducted by Shalon’s co-defendant, Andrei Tyurin, a hacker based in Russia with whom Shalon was in continuous communication.

Shalon and Khokholkov operated their criminal enterprises and various businesses through a series of different offices. At the time of Shalon’s arrest, there were two offices in Moscow (for pharmaceuticals and Coin.mx); three offices in Israel (for securities manipulation and pump and dump schemes, payment processing, and administration); two offices in the

---

network, including Indian manufacturers of drugs, and U.S.-based warehouses that stored pharmaceuticals to enable overnight delivery within the country. Kholkov was principally responsible for managing the pharmaceutical distribution network, whereas Shalon (with Orenstein’s help) focused his efforts on the casino business, as well as maintaining payment processing.

<sup>2</sup> The Government also separately brought charges in *United States v. Anthony Murgio*, No. 15 Cr. 769 (AJN), in which the Government prosecuted multiple U.S.-based individuals for their crimes arising out of the operation of Coin.mx, an unlicensed Bitcoin exchange that was owned by Shalon and Khokholkov but was created and run by Anthony Murgio, a Florida resident and Aaron’s friend since college. Anthony Murgio pleaded guilty and was sentenced by Judge Nathan principally to 66 months’ imprisonment; his co-defendants Trevon Gross and Yuri Lebedev were found guilty after a four-week jury trial and were sentenced by Judge Nathan principally to 60 and 16 months’ imprisonment, respectively.

Honorable Laura Taylor Swain

November 3, 2020

Page 3

Ukraine (for support of the gaming business, pharmaceuticals, and the detection of fraud in their payment processing schemes); an office in Macedonia (for gaming and banking); and an office in Serbia (for marketing), with plans of opening further offices in Azerbaijan, Georgia, Costa Rica and elsewhere.

**A. Unlawful Online Gambling Business**

From approximately 2007 through his arrest in July 2015, Shalon owned and operated multiple unlawful internet casinos that accepted bets from U.S.-based customers in violation of United States law. Shalon employed hundreds of employees in multiple countries in connection with this business. To promote the online casinos, Shalon and others engaged in large-scale email spam promotions, often using lists of potential customers that had been obtained through hacking customer data from major companies, including U.S.-based companies that provided email marketing services for other businesses. The vast majority of the players who used his online casinos were from the United States, as was true of most online gambling sites. At the time that Shalon began his online casinos, U.S.-based financial institutions refused to process online gambling transactions.<sup>3</sup> Specifically, U.S.-based financial institutions refused to process credit card transactions from merchant accounts with a particular merchant category code (7995, which is for Betting/Casino Gambling).<sup>4</sup> Thus, in order to accept money from U.S.-based customers of the online casinos, and as is further described below, Shalon's casinos had to miscode the transactions as innocuous transactions in order to deceive credit card companies into processing these gambling transactions. Shalon also engaged in hacks and cyberattacks against other internet gambling businesses and an internet gambling software company in order to steal customer information, as well as to secretly read the emails of these companies' executives. In addition, Shalon directed distributed denial of service ("DDoS") attacks against competitor internet gambling businesses in order to temporarily shut down these businesses.

Orenstein primarily served as Shalon's accountant for the casino business during the relevant time period, and was in charge of overseeing financial transactions relating to the casino brands, including online deposits and withdrawals by the casino customers, the tracking of revenues and expenses, and the distribution of profits to various offshore accounts. From evidence collected over the course of the investigation, including data taken from Orenstein's laptop, the Government has determined that the total volume of Shalon's casino business from

---

<sup>3</sup> In October 2006, pursuant to the Unlawful Internet Gambling Enforcement Act of 2006 (UIGEA), it became illegal to accept credit, electronic fund transfers, checks, or any other payment involving online gambling from U.S.-based players. Nevertheless, even before this time, U.S. issuing banks deemed online gambling a high-risk business for payment processing purposes, and thus miscoding of unlawful internet gambling transactions to evade declination by U.S. issuing banks began even prior to the passage of the UIGEA.

<sup>4</sup> A merchant category code, or MCC, is a four-digit number assigned to a type of business by credit card companies (e.g., Visa and Mastercard), which reflects the primary category in which a merchant does business. It serves as a classification of the type of goods or services that a particular merchant provides.

Honorable Laura Taylor Swain  
November 3, 2020  
Page 4

approximately January 2008 to June 2015 was approximately \$438,711,306, of which approximately \$386,065,949 represents illegal casino volume from U.S. customers. Of that volume, the Government further has estimated that Shalon's enterprise received approximately \$80,112,953 in illegal casino profits from approximately January 2008 to June 2015.

**B. Illegal Payment Processing and Bribery of Foreign Bank Officials**

Shalon and Khokholkov facilitated the processing of credit and debit card transactions for major credit card networks (such as Visa, Mastercard, and American Express) in furtherance of their various criminal businesses, including gambling, online pharmaceuticals, and Coin.mx, the unlicensed bitcoin exchange. Payment processing grew in importance as a component of Shalon's businesses once U.S.-based financial institutions stopped processing for online gambling. As a result, Shalon, Khokholkov, Orenstein, and their co-conspirators would miscode the online gambling transactions in order to deceive credit card companies into processing these transactions. Among other things, Shalon, Khokholkov, Orenstein, and their co-conspirators would set up and manage a series of front companies and websites, designed to look as though the front companies were innocuous online merchants selling items like pet toys and clothing. They would then open merchant accounts in the name of the front companies at financial institutions, and miscode credit and debit card transactions for their criminal activities as though they were for the front company.

As it became more difficult to successfully miscode the transactions, Shalon and Khokholkov sought a more stable solution to ensure that his various criminal enterprises could continue to accept online payments. Consequently, Shalon and his co-conspirators turned to bribing bank officials at five different banks in Azerbaijan and then using those banks to process credit card transactions for various criminal businesses. Orenstein had relationships with these bribed Azerbaijani banking officials, and corresponded regularly with them about the payment processing, including regarding fraud that was being detected in the payment processing, such that Orenstein and Shalon could work to decrease chargebacks<sup>5</sup> and/or open new merchant accounts for credit card processing when necessary.

---

<sup>5</sup> A chargeback is a demand by a credit card company for a retailer to make good on or refund the loss on a fraudulent or disputed transaction as reported by a consumer. In credit card processing for so-called "high risk" merchants (such as online gambling, pharmaceuticals, bitcoin purchases, and pornography), there is a high rate of chargebacks, where the credit card holder disputes the charge and demands a refund. Credit card companies generally require that merchant accounts maintain a chargeback rate below a certain percentage, and also impose a "rolling reserve" requirement for high risk processing, where a portion of the credit card volume processed is secured to cover the potential risk of future chargebacks.

Honorable Laura Taylor Swain  
 November 3, 2020  
 Page 5

In addition, Shalon, Khokholkov, and Tyurin worked together to hack into and monitor the internal communications and systems of a merchant risk intelligence firm based in Washington State, who worked to audit fraudulent online payment processing on behalf of the major credit card networks. After Tyurin successfully gained access into the firm's networks, Shalon, Tyurin, and Khokholkov would work together to download information from the firm, including internal communications and lists of credit card numbers being used by the firm to audit online merchants, in an effort to ensure their fraudulent scheme would not be uncovered. As a result of Tyurin's hacking of the firm, Shalon, Khokholkov, and their co-conspirators had persistent access to lists of credit card numbers and identifiers that were being used by auditors to run test transactions in order to identify miscoding and fraudulent transactions. Because Shalon and Khokholkov was able to conduct countersurveillance in furtherance of their payment processing scheme in this manner, their criminal organization was able to stay one step ahead of the auditors and continue their fraudulent payment processing scheme.

Shalon and Khokholkov also jointly owned Coin.mx, the unlicensed Florida- based bitcoin exchange that was run by Anthony Murgio and others in the United States. Azerbaijani banks knew that the credit card networks did not want to process bitcoin transactions. Nevertheless, Shalon, Khokholkov, and Orenstein used these banks to process for Coin.mx, and coded the transactions as 6051 (which is "Non-Financial institutions - Foreign Currency, Money Orders (not wire transfer) and Travelers Cheques"), at the banks' request.

From evidence collected over the course of the investigation, including from Shalon and Orenstein's laptops, the Government conservatively estimates that the payment processing operations run by Shalon reaped profits of \$17,848,138 for the period of March 2011 to April 2015. Of this figure, Shalon himself received approximately \$8,656,347.

### **C. Online Pharmaceuticals**

Shalon and Khokholkov jointly owned RxPartners, one of the largest online pharmaceutical affiliate networks. During the relevant period, RxPartners sold generic versions of patented pharmaceuticals, mainly erectile dysfunction drugs Viagra and Cialis. RxPartners had its own distribution network, including Indian manufacturers of drugs, and U.S.-based warehouses that stored pharmaceuticals to enable overnight delivery within the country. Although Shalon was Khokholkov's partner in the enterprise, Khokholkov was responsible for managing the pharmaceutical distribution network, whereas Shalon was charged with maintaining its payment processing. Because RxPartners was having difficulty maintaining payment processing for U.S.-based customers, Shalon built a "whitelisting"<sup>6</sup> system for payment processing for Khokholkov, which analyzed user behavior, IP addresses, network scans, time zones, and other factors to prevent auditors from detecting that the transactions at issue were for

---

<sup>6</sup> In the context of cybersecurity, a "whitelist" generally refers to a list or register of entities that have been provided a particular privilege, service, mobility, access, or recognition. As used here, Shalon and his co-conspirators created a payment processing system designed only to let true customers—as opposed to auditors—execute credit card transactions.

Honorable Laura Taylor Swain  
November 3, 2020  
Page 6

illegal counterfeit pharmaceuticals. The system also integrated data that was retrieved from the merchant risk intelligence firm which had been hacked at Shalon's direction, as described above, such as lists of credit card numbers that were used by auditors for Visa and Mastercard in order to identify fraudulent merchant accounts.

#### **D. Stock Pump-and-Dump**

In approximately January 2012, Shalon agreed to begin working with Aaron on the stock manipulation schemes. At first Aaron sought to buy email addresses from Shalon to use in stock promotion schemes, but Shalon stated he would only provide Aaron with the data if Aaron partnered with him for purposes of the promotion. Aaron then left his previous partner, and he and Shalon conducted pump-and-dumps of penny stocks together. Aaron would select particular companies whose stock could be promoted, and would help craft the promotional materials (which included material misrepresentations about the companies being promoted) as well as company names (such as "Stock Castle" and "Wall Street Penny Stocks") through which Shalon and Aaron would conduct the marketing campaigns. Aaron would also interact with English-speaking parties in furtherance of the operation, including co-conspirators who "controlled the float" (i.e., had control over the free trading shares of the company at issue, so as to enable the market manipulation to occur), copywriters who would generate the promotional materials, and brokerage firms used to execute the trades. Shalon in turn would provide the infrastructure necessary to execute the project, including fraudulently used identities, shell companies, and financial accounts to fund projects. Shalon also would launder the proceeds, as well as handle the promotion of the penny stocks through email campaigns, websites, and phone banks. Aaron also did research on various companies for Shalon to hack, including the U.S. financial companies, with the understanding that customer lists from those companies could be used in the promotion of the stocks. Aaron provided online accounts to Shalon for the banks and companies that were to be targeted, such that Shalon and Tyurin could use the accounts to perform network reconnaissance in furtherance of the hack.

According to Shalon, the total volume of stock traded by Shalon, Aaron, and their co-conspirators through the project was approximately \$20 million, and the overall income from the manipulation scheme was approximately \$9 million dollars.

#### **E. Binary Options**

In parallel with his gambling business, Shalon was also an investor and owner of businesses relating to binary options.<sup>7</sup> Shalon first became involved in the binary options

---

<sup>7</sup> Generally, binary options refer to financial options in which the payoff is either a fixed amount or nothing. Binary option companies allow individuals to "invest" by purchasing binary call options, which stipulate that the investor receive a specific amount if the particular option expires in-the-money, and loses the "investment" (i.e., the price of the binary call option) if the option does not. In other words, an individual is essentially betting on movements of either stocks or foreign currencies. Because binary option companies are oftentimes operating on the

Honorable Laura Taylor Swain  
November 3, 2020  
Page 7

industry in approximately 2013, when he invested approximately \$2.5 million in a company named Cedar Finance, which was being run at the time by two Polish citizens who were also involved in gambling businesses. Shalon made this investment in exchange for a 50% stake in the company, which would then turn into an even 33.3% split between all three owners once Shalon recouped his investment. However, shortly after Shalon invested in Cedar Finance, his Polish partners were arrested in the UK for having participated in cyberattacks involving a dispute over a gambling company that the Polish partners had previously jointly owned with another individual.<sup>8</sup> After that point, Shalon invested another \$1.5 million of his own money to keep Cedar Finance afloat, as well as to pay for the Polish partners' legal fees and their families' living expenses while they were incarcerated. Within a year, in approximately 2014, he and Khokholkov purchased a 27% stake in Tradeologic, a company that offered the software platform that facilitated other companies' offering of binary trading to customers online. According to Shalon, because Tradeologic did not support U.S.-facing binary options companies, Cedar Finance also stopped offering its binary options services to U.S. customers. The Polish partners were released from prison and rejoined Cedar Finance's operations shortly before Shalon's arrest in July 2015.

With regard to Cedar Finance, Shalon explained that the company used trading bots that would delay actual prices for stocks or currency from posting to the website by a very short period of time (approximately a second). The short delay between market changes in price and what the binary options customer saw online allowed the algorithm used to power the bots to more accurately predict future movements in price for short periods of time over which bets were placed through the purchasing of binary call options by the customers. This allowed the bots to provide purported advice to the customers about which options to purchase. Shalon further explained that there were many mechanisms built into the code that would induce customers to continue to make deposits. These included, for example, a series of call options that would be suggested by the bots to consumers which would yield gradual net gains for a period of time, followed by a large crash and near total losses to the customers, right when they started to contemplate making withdrawals from their accounts at Cedar Finance. Shalon described this as a fraud and a Ponzi-like scheme, in which a series of bets which yielded consistently stable returns then resulted in an engineered complete loss to the consumer. Deposits were made by consumers in the same matter as described above in the context of gambling (i.e., through wire transfers and miscoded credit card transactions).

According to Shalon, he never fully recuperated his investment in the binary options businesses prior to his arrest. He estimates that during the two years he was involved in Cedar Finance, the company received between \$1-4 million in deposits a month, with approximately \$2 million in profits.

---

Internet, and outside of financial regulatory frameworks, they are prone to fraud at the expense of the consumers.

<sup>8</sup> Shalon admits he had a role in the series of cyberattacks that occurred between various competitors in the gambling market, including the rivalries that led to this incident.

Honorable Laura Taylor Swain  
 November 3, 2020  
 Page 8

#### **F. Computer Hacking In Furtherance of Criminal Businesses**

Approximately eight to nine years prior to his arrest, Shalon was approached by an individual on ICQ (an internet chat protocol) who indicated he had data to sell to Shalon for purposes of spamming, for which Shalon paid \$50,000 through a Russian-based money transfer business. Over time, Shalon learned that this individual's name was "Andrei," and he met with Andrei a few times in person, including in Russia, Ukraine, Georgia, and Israel. At first, Shalon paid "Andrei" to help infiltrate various gaming servers of his competitors, in order to collect data (including contact lists for users for purposes of spamming), which Shalon would then either use or sell to others. Shalon would provide the network infrastructure "Andrei" needed to conduct his work on behalf of Shalon. At Shalon's request, "Andrei" hacked into iContact, a large internet marketing company based in North Carolina that provides email marketing services to its customers, and stole approximately 1.5 billion email addresses. "Andrei" also hacked into various companies within the gaming industry, news websites such as [REDACTED] (a financial investment newsletter), and various financial sector companies, including [REDACTED], and others. These financial sector hacks resulted in the theft of data for over 100 million customers, which at the time included the largest theft of customer data from a U.S. financial institution. In addition, "Andrei" also decrypted passwords and executed trades at Shalon's direction at various of these companies. Shalon estimates that "Andrei" executed approximately \$30,000 to \$50,000 worth of trades in hacked accounts. Shalon met "Andrei" several times in person, and "Andrei" traveled to Israel and the Ukraine to meet with Shalon. After the hack into [REDACTED], Shalon and Tyurin monitored the news reporting regarding the hack, and undertook to delete and destroy online infrastructure and evidence linking the two to the attack, as a means to undermine law enforcement efforts.

At the time of Shalon's arrest, the Government seized an unencrypted USB drive found at Shalon's home. That USB drive contained chats in Russian between Shalon and an individual who appeared to be the hacker, in which they described, among other things, the companies they hacked from approximately 2013 to mid-2014. Those conversations also included information regarding flights that the hacker had taken to meet Shalon in other countries. By comparing border crossing data and flight manifests, the Government identified Andrei Tyurin as the hacker. [REDACTED]

[REDACTED] the Government was further able to confirm that Andrei Tyurin is the hacker's full identity. Tyurin was subsequently arrested, extradited, and pleaded guilty to charges related to his role in the hacking schemes.

#### **G. Money Laundering**

In order to maintain the financial operations of the criminal enterprise, Shalon and his co-conspirators would set up shell companies and opened bank accounts in various countries, including in the United States, Georgia, Latvia, Azerbaijan, Cyprus, and Switzerland. Specifically, Shalon, Khokholkov, and their associates had recruited various individuals to act as

Honorable Laura Taylor Swain  
November 3, 2020  
Page 9

“nominees,” whose names and identification documents were used with their consent to open accounts and serve as directors to a variety of shell companies incorporated in places such as the British Virgin Islands and Cyprus. These nominees would provide copies of their identification documents, execute and provide requisite documents, and meet with financial institutions, if necessary, so as to facilitate the use of the various accounts to launder money and proceeds of Shalon’s various criminal schemes. On occasion, however, Shalon and his co-conspirators would also use the identities without the consent of their owners, and falsify documents when necessary to keep accounts open and execute transactions. In particular, Shalon and his co-conspirators would occasionally pretend to be various of these “nominees” while corresponding with financial institutions and securities firms, and would also create or procure fraudulent identity documents, including passports, utility bills, and resumes, if necessary.

#### **H. Miscellaneous Other Criminal and Bad Acts**

[REDACTED]

Shalon also was involved in a physical altercation at [REDACTED] involving other inmates. A review of the paperwork and the video of the incident establishes that Shalon and another inmate engaged in a verbal argument about who could use a telephone in the dorm. This resulted in Shalon stepping toward the other inmate and aggressively touching his forehead against the forehead of that inmate. The verbal argument continued, and it escalated into Shalon being assaulted by a group of other inmates. After that incident, Shalon was placed in RHU and subsequently has been transferred [REDACTED]. Shalon’s description of this incident was truthful, and was consistent with the videotape, incident reports, and interviews conducted of witnesses and others involved in the altercation.

Shalon states that he has had no prior arrests or convictions. Based on available information, it does not appear that Shalon was engaged in any other criminal activity beyond what is described above.

Honorable Laura Taylor Swain  
 November 3, 2020  
 Page 10

### **Shalon's Cooperation and Section 5K1.1 Factors**

Section 5K1.1 of the Guidelines sets forth five non-exclusive factors that sentencing courts are encouraged to consider in determining the appropriate sentencing reduction for a defendant who has rendered substantial assistance. *See* U.S.S.G. § 5K1.1(a). The application of these factors to Shalon's cooperation is set forth below.

#### **A. Timeliness of Shalon's Assistance (U.S.S.G. § 5K1.1(a)(5))**

On July 21, 2015, Israeli law enforcement arrested Shalon and his co-conspirator, Ziv Orenstein on charges relating to the securities "pump and dump" scheme, and executed search warrants at both residences.<sup>9</sup> [REDACTED]

[REDACTED] confirmed both that Shalon had directed intrusion activity against U.S. financial sector companies, and that Shalon's organization had participated in a vast array of criminal activities, as detailed further below. Accordingly, the Government brought superseding charges against Shalon, Aaron, and Orenstein, which were announced in November 2015. Shalon was also charged by the United States Attorney's Office for the Northern District of Georgia, who along with the FBI's Atlanta Office were investigating the hack of [REDACTED] (a victim company located in their District) at the time that the [REDACTED] hack occurred, and separately brought charges relating to the hacks of [REDACTED]. *See* Indictment, *United States v. Shalon*, 15 Cr. 393 (N.D. Ga.).

[REDACTED] Shalon consented to extradition to the United States on both the S.D.N.Y. and the N.D. Ga. charges, and was extradited to the United States in June 2016. Prior to his being signed up as a cooperating witness, the Government met with Shalon over a dozen times, during which Shalon provided a detailed account of his various criminal activities, as well as the criminal activities of numerous others.

[REDACTED] Shalon's account was corroborated both by evidence that had been gathered by the

---

<sup>9</sup> A third co-conspirator, Joshua Samuel Aaron (a U.S. citizen) was also charged, but Aaron, who had previously lived in Israel, was in Russia at the time of the planned arrests without firm plans to return. As is discussed further below, in May 2016, Aaron was arrested in Russia in light of the fact that there was an Interpol Red Notice for his arrest, and was charged with having violated Russian immigration laws. He was ordered deported in Russia and arrived on December 14, 2016 in the District.

Honorable Laura Taylor Swain  
 November 3, 2020  
 Page 11

FBI and the USSS over the course of their investigation, as well as documents and emails found on his electronic devices [REDACTED]

On April 27, 2017, Shalon pleaded guilty to cooperation agreement pursuant to a cooperation agreement to Counts One through Twenty Three of the indictment docketed S1 15 Cr. 333 (LTS), and to Counts One through Ten of the indictment docketed 17 Cr. 254 (LTS), which were the charges brought by the United States Attorney's Office for the Northern District of Georgia for which Shalon agreed to transfer to this District pursuant to Federal Rule of Criminal Procedure 20. Shalon also agreed to pay forfeiture and restitution as ordered by the Court.

**B. Truthfulness, Completeness, and Reliability of Shalon's Information (U.S.S.G. § 5K1.1(a)(2))**

With regard to the "truthfulness, completeness, and reliability" of the defendant's information, *see* U.S.S.G. § 5K1.1(a)(2), over the course of over a dozen meetings with Shalon prior to his being signed up as a cooperating witness, Shalon was forthcoming and truthful about his own criminal conduct and that of other individuals involved in the organization's various criminal schemes. Expressing remorse for his conduct, Shalon approached his cooperation with diligence, a positive attitude, and with the goal of doing everything he could to account for his crimes. The information provided by Shalon was corroborated by documentary evidence collected over the course of the investigation, including information found on Shalon's and Orenstein's devices, and was helpful in allowing the Government to better understand the mechanics of Shalon and Khokhlov's criminal schemes, particularly in illuminating the financial infrastructure that was used by Shalon and the organization.

**C. Significance and Usefulness, and Nature and Extent of Shalon's Assistance (U.S.S.G. § 5K1.1(a)(1), (3))**

With regard to the "significance and usefulness of the defendant's assistance," U.S.S.G. § 5K1.1(a)(1), and the "nature and extent of the defendant's assistance," *see* U.S.S.G. § 5K1.1(a)(3), it is the Government's view that Shalon's assistance, both in this case and in others, has been extraordinary. [REDACTED]

In total, Shalon has provided information that has been used in [REDACTED] FBI investigations, in the New York Field Office as well as other offices across the country. In many instances, Shalon's assistance has helped substantively move investigations forward, including by [REDACTED]

Honorable Laura Taylor Swain

November 3, 2020

Page 12

[REDACTED]

Among the most significant examples of Shalon's assistance to date are as follows:

- [REDACTED]
- [REDACTED]
- Shalon helped facilitate the repatriation of his various criminal assets to the United States, including most notably the transfer of over \$74 million from Switzerland. Shalon not only agreed to forfeit these funds, but also had to have multiple conversations with representatives at the Swiss bank to facilitate the funds. As it is usually difficult to forfeit criminal proceeds from Switzerland, Shalon's cooperation in this regard will result in the unusual situation whereby several of his victims will be made whole from the injury they suffered as a result of the hack.
- [REDACTED]

Honorable Laura Taylor Swain

November 3, 2020

Page 13

[REDACTED]

- [REDACTED]

[REDACTED]

- [REDACTED]

Honorable Laura Taylor Swain

November 3, 2020

Page 14

[REDACTED]

[REDACTED]

- [REDACTED]

- [REDACTED]

- [REDACTED]

- [REDACTED]

[REDACTED]

- [REDACTED]

---

[REDACTED]

Honorable Laura Taylor Swain  
November 3, 2020  
Page 15

[REDACTED]

- [REDACTED]

- [REDACTED]

- [REDACTED]

- [REDACTED]

Honorable Laura Taylor Swain

November 3, 2020

Page 16

[REDACTED]

- [REDACTED]

- [REDACTED]

- [REDACTED]

In sum, Shalon has provided substantial assistance to the Government's efforts to investigate and prosecute both the individuals involved in Shalon's criminal organization, as well as multiple other criminal investigations. [REDACTED]

[REDACTED]

Furthermore, Shalon has continued to abide by the terms of his pretrial supervision since his release in 2017.

Honorable Laura Taylor Swain  
November 3, 2020  
Page 17

**D. Danger or Risk of Injury to Shalon or his Family Resulting from his Assistance (U.S.S.G. § 5K1.1(a)(1), (4))**

[REDACTED]

**Conclusion**

In light of the facts set forth above, and assuming that Shalon continues to comply with the terms of his cooperation agreement, the Government intends to request at sentencing that the Court sentence Shalon in light of the factors set forth in Section 5K1.1 of the Guidelines. In addition, because of the sensitive nature of the information contained in this letter, including details of the defendant's cooperation [REDACTED], the Government respectfully requests that this letter be filed under seal.

Respectfully submitted,

AUDREY STRAUSS  
Acting United States Attorney

By: /s/  
Eun Young Choi  
Assistant United States Attorney  
Tel: (212) 637-2187

cc: Paul Shechtman, Esq. (by e-mail)

The sealing request is granted as to the foregoing sentencing submission, for the reasons stated above. The parties must make a joint status written report by May 1, 2021, and each May 1 thereafter, as to whether (and why) continued sealing is necessary.

SO ORDERED.

12/1/2020

/s/ Laura Taylor Swain, USDJ